Effective Subtractive Security

By Dean Webb

Reactive vs Subtractive 1

- Reactive: Aaaaah we are under attack by thousands of mighty riders and our weapons are designed to deal with footmen WHAT WILL WE DO??? Order more pikes!!! And pray!!!

- Subtractive: We’re in a fort. Lock the door.

Reactive vs Subtractive 2

- Reactive: There are SO MANY kinds of bacteria and NO ONE thing will kill them all and sometimes the symptoms don’t present themselves until DAYS after an infection and if your house isn’t stocked fully with a full range of remedies you have NO HOPE against a bacterial infection leaving you crippled!!! Or dead!!!

- Subtractive: Wash your hands before and after certain events.

Reactive vs Subtractive 3

- Reactive: Project Glasswing can find thousands of zero-days and AI tools can build exploit kits in a matter of hours!!! We can’t patch fast enough!!! All our base is belong to THEM!!! AIIIEEEE!!!

- Subtractive: How about we not panic and block pathways?
  - 10 high-impact, low-friction endpoint and network subtractions
  - Equivalent of locking the door and washing hands – quiet, calm responses that we know will work

Subtractive Top 10

- https://subtractivesecurity.com/subtractive-top-10/
- Briefings, Guidance, Top 10 List, Core Doctrines
- Basically, erase paths to subtract risk.
- https://www.amazon.com/Science-Silence-Subtractive-Security-Physics/dp/B0GWN47V1J
- **The Science of Silence: Subtractive Security and the Physics of Defense** by Christopher Frenz
- 74 pages, quick read, lots of great, usable content

Subtractive Top 10

- ***S01: Process Tree Integrity*** Prevent browsers and office suites from launching system shells (cmd, powershell)
- ***S02: Protocol Extinction*** Remove legacy discovery protocols (NTLM, LLMNR, NetBIOS)
- ***S03: Execution Locality*** Block unsigned binary execution from user-writable directories (%AppData%, %Temp%)
- ***S04: Lateral Path Erasure*** Disable p2p admin protocols on non-servers (RDP, SMB)

Subtractive Top 10

- ***S05: Credential Guardrails*** Enforce LSA protection and disable credential caching (WDigest)
- ***S06: Scripting Host Lockdown*** Disable non-admin access to wscript.exe and cscript.exe across the enterprise
- ***S07: Surface Area Pruning*** Decommission non-essential OS features by default (XPS, SMBv1, Fax, Print spooler)

Subtractive Top 10

- ***S08: Identity Path Silencing*** Restrict use of local Admin accounts and remove them from network-accessible groups
- ***S09: Shell Contextualization*** Enforce Constrained Language Mode for PowerShell – prevents living off the land techniques for attackers
- ***S10: Egress Determinism*** No more outbound “allow all” – traffic must be authenticated, proxy-only egress… *null route* everything else

Non-Conductivity

- Imagine how many Star Trek episodes would collapse if touching a computer panel didn’t automatically grant root access…
- Star Wars would end after 45 mins when either the old password didn’t work or connecting to a droid access port didn’t grant root access…
- The Subtractive Top Ten provide deterministic boundaries that break conductivity
  - Vulnerabilities will always be “sparking”
  - Non-conductive enterprises will block sparks from the “oxygen” of a valid attack path

Measure Security Differently

- Attacks blocked = you were still attacked :-(
- Patches applied = you will apply more patches next week :-(
- Vulnerabilities found = you know what the attacker knows :-(
- Path removal eliminates one or more TTPs :-)
- Path removal means a new zero-day that relies on a TTP you have blocked will not be a threat :-)
- Path removal changes alerts from constant noise to periodic signals with true meaning :-D

Permanent Patching Backlog

- AI will discover and chain vulns faster than we can review, test, and deploy patches
- Even if AI writes all the patches, we still have maintenance windows for applying them
- What good is finding a million vulnerabilities if we can’t safely fix a million vulnerabilities?
- Patching backlog is a mathematical certainty – written after vuln found, often after exploit exists – can no longer be primary defense

Vulnerabilities != Risk : ***Paths = Risk***

- Vulnerabilities matter ONLY if they are actionable
  - Control
  - Movement
  - Impact
- All the vulns that AI can write exploits for still require attack paths
  - When do we need our browsers to launch PowerShell?
  - When does a local user need to use WMI commands on another user?
  - When do we need an untrusted binary to access credential memory?
  - When do we need ads to run? Block ‘em… :-D

Final Thoughts

- Sound architecture with paths removed is the security we want and the security users want.
- AI did not break security – it exposed which parts never scaled.